



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/583,588	06/19/2006	Benjamin Morin	33901-201PUS	6747
27799	7590	03/05/2008	EXAMINER	
COHEN, PONTANI, LIEBERMAN & PAVANE			ABRISHAMKAR, KAVEH	
551 FIFTH AVENUE				
SUITE 1210			ART UNIT	PAPER NUMBER
NEW YORK, NY 10176			2131	
			MAIL DATE	DELIVERY MODE
			03/05/2008	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/583,588	MORIN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	KAVEH ABRISHAMKAR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 19 June 2006.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-9 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-9 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | Paper No(s)/Mail Date. _____ .                                    |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>06/19/2006</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application |
|   | 6) <input type="checkbox"/> Other: _____ .                        |

## DETAILED ACTION

1. This action is in response to the communication filed on June 19, 2006. Claims 1-7 were originally filed for consideration. A preliminary amendments to the claims was filed on June 19, 2006, adding claims 8-9.
2. Claims 1-9 are currently pending consideration.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 7 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because the claims are interpreted as being purely software per se. Data structures or computer programs not claimed as embodied in computer-readable media are descriptive material per se and are not statutory because they are not capable of causing functional change in the computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. Claimed computer programs do not define any structural and functional interrelationship between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See

Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions (see Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility: Annex IV).

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-9 are rejected under 35 U.S.C. 102(a) as being anticipated by Julisch's "Clustering Intrusion Detection Alarms to Support Root Cause Analysis."

Regarding claim 1, Julisch discloses:

A method of automatically classifying alerts issued by intrusion detection sensors (11a, 11b, 11c) of an information security system (1) for producing collated alerts, each alert being defined by a plurality of qualitative attributes (a.sub.1, . . . a.sub.n) belonging to a plurality of attribute domains (A1, . . . , An) (page 449, paragraph 2, lines 3-5) each of which has a partial order relationship, which method comprises the following steps:

organizing the attributes belonging to each attribute domain into a hierarchical structure including levels defined in accordance with the partial order relationship of the

attribute domain, the attribute domains thus forming hierarchical structures (page 449, paragraph 4, lines 1-9: "*generalization hierarchy*");

constructing for each alert issued by the intrusion detection sensors (11a, 11b, 11c) a trellis specific to that alert by generalizing each alert in accordance with each of its attributes and at all the levels of the hierarchical structure (page 453, paragraph 7, lines 1-6 - page 453, paragraph 1, lines 1-2: "*generalized attribute values*"), the specific trellis including nodes corresponding to alerts linked to each other by arcs so that each node is linked to one or more parent nodes and/or to one or more child or descendant nodes (page 454, paragraph 2, lines 13-20: "*via a common parent*");

iteratively merging each specific trellis into a general trellis (page 456, paragraph 7, lines 1-13: "*repeatedly generalizes the alarms*");

identifying collated alerts in the general trellis by selecting the alerts that are simultaneously the most pertinent and the most general in accordance with statistical criteria and according to their attributes belonging to lower levels of the hierarchical structures (page 457, paragraph 1, lines 1-17: "*each generalized alarm a represents an alarm cluster*"); and

supplying the collated alerts to an output unit (23) of an alert management system (13) in order to provide an overview of all the alerts issued by the intrusion detection sensors (11a, 11b, 11c) (page 457, paragraph 1, lines 14-17: "*generalized alarm*").

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Julisch discloses:

The method according to claim 1, wherein the construction of a specific trellis includes the following steps:

for any generalizable attribute of a given alert, recovering the generalized value of that attribute from its hierarchical structure to form a new alert more general than said given alert (page 457, paragraph 1, lines 11-16): “*original alarms*”;

adding a new node to the specific trellis corresponding to the new alert and adding an arc going from the new node of the new alert to the node of the given alert (page 457, paragraph 1, lines 11-16: “*merge identical alarms into a single generalized alarm*”); and

adding missing arcs going from the parent nodes of the given alert resulting from the generalization of the given alert in accordance with its other attributes to the node of the new alert (page 457, paragraph 1, lines 11-16: “*merge identical alarms into a single generalized alarm*”).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Julisch discloses:

The method according to claim 1, wherein merging a given specific trellis into the general trellis includes the following steps:

selecting a first node corresponding to a first alert belonging to the given specific trellis and a second node corresponding to a second alert belonging to the general

trellis (page 450, paragraph 3, lines 1-6: *an "alarm cluster" is interpreted as a general trellis, and a group of "generalized alarms" is a general trellis*);

eliminating all the arcs coming from the parent nodes of an offspring node of the first node if said offspring node belongs to said general trellis (page 457, paragraph 1, lines 1-16, *replace the  $A_i$  values of all alarms in  $T$  by their parents values in  $G_i$* ); and

adding said offspring node and all its descendants to the general trellis if said offspring node does not belong to the general trellis (page 457, paragraph 1, lines 1-16, *merge identical alarms into a single generalized alarm*).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Julisch discloses:

The method according to claim 1, wherein a pertinent alert is identified when each of the sets of offspring nodes of the pertinent alert resulting from specialization of that alert in accordance with each of its attribute domains is homogeneous and when the number of elements constituting each of said sets of offspring nodes of the pertinent alert is greater than a threshold value (page 455, paragraph 2, lines 1-8: *"small heterogeneity value implies that there exists a generalized alarm"*, page 457, paragraph 3, lines 1-4).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Julisch discloses:

The method according to claim 1, wherein the collated alerts are associated with different groups of alerts issued by the sensors so that the groups are not mutually exclusive (page 457, paragraph 1, lines 8-16)

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Julisch discloses:

The method according to claim 1, wherein the attribute domains from the following sets: alert identifiers, attack sources, attack targets, and attack dates (page 460, paragraph 3-5: "*hierarchies for numerical, time, and string-valued attributes*").

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Julisch discloses:

A computer program designed to execute the method according to claim 1 when it is executed by the alert management system (13) (page 445, paragraph 4, lines 1-7).

Regarding claim 8, Julisch discloses:

Alert management system for automatically classifying alerts issued by intrusion detection sensors for producing collated alerts, each alert being defined by a plurality of qualitative attributes (a.sub.1, . . . , a.sub.n) (page 449, paragraph 2, lines 3-5) belonging to a plurality of attribute domains (A1, . . . , An) each of which has a partial order relationship, which system comprises:

processor means for organizing the attributes belonging to each attribute domain into a hierarchical structure including levels defined in accordance with the partial order relationship of the attribute domain, the attribute domains thus forming hierarchical structures (page 449, paragraph 4, lines 1-9: "*generalization hierarchy*");

processor means for constructing for each alert issued by the intrusion detection sensors a trellis specific to that alert by generalizing each alert in accordance with each of its attributes and at all the levels of the hierarchical structure (page 453, paragraph 7, lines 1-6 - page 453, paragraph 1, lines 1-2: "*generalized attribute values*"), the specific trellis including nodes corresponding to alerts linked to each other by arcs so that each node is linked to one or more parent nodes and/or to one or more child or descendant nodes (page 454, paragraph 2, lines 13-20: "*via a common parent*");

processor means for iteratively merging each specific trellis into a general trellis (page 456, paragraph 7, lines 1-13: "*repeatedly generalizes the alarms*");

processor means for identifying collated alerts in the general trellis by selecting the alerts that are simultaneously the most pertinent and the most general in accordance with statistical criteria and according to their attributes belonging to lower levels of the hierarchical structures (page 457, paragraph 1, lines 1-17: "*each generalized alarm a represents an alarm cluster*"); and

processor means for supplying the collated alerts to an output unit (23) in order to provide an overview of all the alerts issued by the intrusion detection sensors (page 457, paragraph 1, lines 14-17: "*generalized alarm*").

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Julisch discloses:

Information security system comprising intrusion detection sensors and an alert management system according to claim 8 (page 445, paragraph 4, lines 1-7).

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/  
Examiner, Art Unit 2131

/K. A./  
Examiner, Art Unit 2131  
February 27, 2008